Michael Best

AT A GLANCE

Preparing for the California Consumer Privacy Act

The California Consumer Privacy Act of 2018 (CCPA) is a game-changing law that some estimate will impact more than 500,000 U.S. companies that do business with residents of the State. Its requirements go into effect no later than July 1, 2020 and potentially sooner.

Does the CCPA Apply to You?

Although the CCPA was passed in California, it could apply to your organization even if it is not located in California. The new law applies to any for-profit business that collects personal information from California residents and meets one or more of the following conditions:

- Has an annual gross revenue of more than $25 million;
- Annually buys, receives, sells, or shares for commercial purposes the personal information of 50,000 or more California consumers, households, or devices; or
- Derives half or more of its yearly revenue from selling California consumers' personal information.

In addition, the CCPA applies to any entity that controls or is controlled by a business that is covered by the CCPA, if it shares common branding with that covered entity.

Notably, the CCPA does not apply to protected health information that is collected by a covered entity or business associate subject to HIPAA, and most of the CCPA does not apply to personal information collected, processed, sold, or disclosed by a financial institution pursuant to GLBA. The CCPA may, however, apply to these organizations with respect to other information that they process.

Who Does the CCPA Protect?

The CCPA protects consumers. A consumer is defined broadly to include any California resident, which means the CCPA also applies to employees. Employers should be prepared to treat California employee data in accordance with the CCPA.

Michael Best

What Information is Covered?

The CCPA applies to the personal information of California residents. Personal information is defined broadly to include information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. Personal information therefore includes information that is not necessarily personal information under other U.S. privacy laws, such as IP addresses or information pertaining to the behaviors of a household. The CCPA even goes so far as to include "olfactory information" as a form of personal information.

What Must Businesses do to Comply?

Privacy Notices

Businesses subject to the CCPA must, at or before the point of collection of personal information, inform consumers as to the categories of personal information to be collected and the purposes for which the categories of personal information will be used. If a covered business is selling consumer personal information, the business must also provide a clear and conspicuous link on the business's Internet homepage titled "Do Not Sell My Personal Information," leading to an Internet Web page that enables a consumer, or a person authorized by the consumer, to opt-out of the sale of the consumer's personal information. "Selling" personal information broadly includes any kind of sharing of consumer personal information with a third party for monetary or other valuable consideration.

California consumers may require your organization to honor their rights to their personal information. Consumers may:

- Request from your organization additional information not provided in the initial notice, such as:
  - The categories of sources from which their personal information is collected.
  - The categories of their personal information disclosed for a business purpose or sold.
  - The business purpose for disclosing or selling their personal information.
  - The categories of third parties with whom their personal information is shared or sold.
  - The specific pieces of their personal information collected.
- Opt-out of the sale of their personal information (opt-in is required for children under the age of 16).
- Require deletion of their personal information, subject to multiple exceptions.

Businesses must offer at least two methods for submitting requests and a toll-free number must be one of them.

A business must not penalize a consumer, in terms of service or price, for exercising their CCPA privacy rights BUT a business is permitted in certain cases to incentivize a consumer not to exercise their rights.

Michael Best

What Must Businesses do to Comply?

Enforcement Defense

Businesses subject to threatened or actual AG enforcement actions or private claims from consumers will need to defend themselves and ensure proper communications with regulators and plaintiffs' counsel throughout.

Vendor Management

Businesses subject to the CCPA will need contracts with their vendors and service providers that pass through all applicable CCPA obligations, including providing support for data access and deletion requests.

Cybersecurity

Businesses will need to have reasonable security practices and procedures in place as well as the ability to prove that they are in place.

Training and Tabletops

Businesses are required to train personnel regarding the CCPA's requirements and will need to practice how they will actually comply (e.g., what processes will a business follow to honor a deletion request and which individuals, in which functions, are responsible for executing against the request).

Data Mapping

Businesses will need to understand what personal information they have, where it is located, how it is used, when it is shared, for what purposes it is shared, and with whom it is shared in order to publish accurate privacy notices and honor the rights of California consumers.

How will the Law be Enforced?

Regulator

The California Attorney General has the right to impose civil fines of up to $2,500 for each violation and up to $7,500 for each intentional violation of the CCPA.

Private Cause of Action

The law also includes a private right of action that allows individuals to bring lawsuits against organizations for data breaches resulting from a business's failure to implement reasonable security practices and procedures. The affected party may recover actual damages or statutory damages between $100 and $750 per consumer per incident, or actual damages, whichever is greater (injunctive relief is also available). Businesses will have a 30-day period to cure violations, if a cure is possible. The 30-day clock begins after the business receives notice of an alleged violation. If a business cures within the permitted timeframe, fines and penalties will not be available. Of course, cure will not be possible in many cases.

What's Next?

Businesses that are subject to the CCPA should start preparing now. It will take many businesses one year or more to build out the policies and protocols necessary to comply. Michael Best is here to help.

Michael Best

How We Can Help

Our Privacy & Cybersecurity attorneys can help your business gear up for the CCPA by first determining if and how the new law applies. If it does, we then assist with matters such as:

Consumer Notices

Drafting privacy notices tailored to the context in which information was collected and the contemplated data use and advise on delivery methods. Advising on appropriate opt-out/opt-in notices and mechanisms and in determining when personal information is being sold.

Vendor & Service Provider Management

Reviewing agreements with vendors and other third parties for compliance with CCPA.

Litigation or Regulatory Defense

Defending clients in enforcement actions brought by the California Attorney General or in consumer lawsuits.

Education & Training

Briefing the Board of Directors and other key members of senior management on the CCPA and the business's compliance program. Conducting training and tabletop exercises for relevant personnel.

Cybersecurity

Evaluating your current information security practices and procedures, and conduct information security gap assessments to support the implementation of corrective measures against a reasonableness standard.

Data Management Counseling

Evaluating your data handling practices and assist you in cataloging relevant personal information and mapping data flows, including instances of selling and sharing personal information to enable your organization to comply with its obligations. We will also:

- Build information governance programs to keep data maps current, including internal-facing policies and protocols;
- Prepare procedures for businesses to follow when authenticating and responding to consumer requests, such as opt-outs and data deletion requests.

The Michael Best Advantage

Tech-savvy lawyers

Our lawyers understand the technology solutions that can help clients automate compliance tasks and the pragmatic steps needed to implement them. These include opt-in/opt-out, "right to be forgotten," and data breach notification tools. Our team also has in-house experience so we can answer compliance questions quickly and explain potential risks from a business perspective.

Innovative tools

Our Best Privacy & Cybersecurity Toolkit is an online platform that helps our clients manage compliance with CCPA and other regulations. Clients can take an initial risk assessment using the toolkit at no charge. We then rank their risk level, show where legal action needs to be taken, and create a timeline for compliance.

Fixed fee pricing or other alternative fee arrangements

Some of Michael Best's CCPA compliance services are available on a fixed fee basis or other alternative fee arrangements, which give our clients cost predictability. Pricing is customized for each client's specific circumstances.